

Remarks

The specification has been editorially revised. No new subject matter has been added.

Claims 2, 3, 5, 7, 8 and 10-13 have been amended to define clearly the Applicants' invention. Claims 1, 6 and 14 have been cancelled without prejudice or disclaimer. New claims 16 and 17 have been added to define clearly the Applicants' invention. Claims 2-5, 7-13 and 15-17 are now pending in the present application and are believed to distinguish patentably over the prior art.

In the Final Office Action, the Examiner has rejected claims 1 to 15 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,308,256 to Folmsbee ("Folmsbee") in view of U.S. Patent No. 5,276,738 to Hirsch ("Hirsch"). The Examiner is alleging that the Applicants' invention as defined by these claims would be obvious to one of ordinary skill in view of the teachings of these references. Applicants respectfully submit that the Examiner's objection in view of the cited references is inappropriate for the reasons set forth below.

According to one aspect of the Applicants' invention as defined by new independent claim 16, Applicants provide a method of authenticating a software application loaded on a computer system having an identifier associated therewith. The software application includes an associated engraved signature. The engraved signature is initially blank such that the software application can initially be used on one of a plurality of computer systems but once used on a computer system, it is authenticated for that particular computer system. During the method, when the software application is executed, the engraved signature is read. If the engraved signature is not blank, the identifier is retrieved from the computer system. The retrieved identifier is encrypted using an encryption

method to obtain a computed signature. The computed signature and the engraved signature are compared. Execution of the software application is inhibited if the computed signature does not match the engraved signature. If the engraved signature is blank, the identifier from the computer system is again retrieved. The identifier is encrypted using the encryption method to obtain a computed signature and the computed signature is stored as the engraved signature. The engraved signature is thus generated at the computer system on which the software application is being executed resulting in the software application being authenticated only for that computer system.

The Examiner alleges that Folmsbee discloses the claimed invention except for storing the computed signature as the engraved signature and is alleging that it would be obvious to one of ordinary skill in the art at the time of the invention was made to store the computed signature as the engraved signature. Applicants respectfully submit that the Examiner's commentary is inaccurate.

Folmsbee discloses a configurable processor for processing (CPU) computer programs that are selectable operable thereon. Each CPU chip produced, according to the Folmsbee system, has an instruction set that can be different from the instruction set of any other processor. In the Folmsbee system, data is not descrambled by a standard microprocessor, rather the microprocessor is configured to execute particularly scrambled code. Once the processor is configured in a particular way, in order to use the particular configuration, it is necessary to compile program instructions which are modified in order to be executable by the particular modified processor. As will be appreciated from the above discussion, the Folmsbee system requires that both the processor and the software application be configured specifically for use with one another.

To that end, as stated at column 15, beginning at line 42, the CPU 11 located in the user's computer device 171 receives a key from a remote key server 173 and that key is functional for that particular CPU 11. The user is able to

obtain from the key server 173 for storage in key memory 175 via a public network 177 such as the Internet or a satellite broadcast. The key is only functional when applied to the CPU 11 having a particular identifier 179. This permits program information to be made freely available from a program server 181, and may also be transmitted through public network channels, such as network 177. By use of public key cryptography, the use of the key is secure. Other users represented by blocks 185 have access to the program information from the program server but must obtain corresponding keys of that program information.

Hirsch discloses a mechanism for controlling the use of software packages including means for taking an input binary value and generating a unique key value as well as performing a reverse operation. The mechanism includes a scrambler which includes storage for an input binary number and an associated memory array having a number of multibit container locations. Each of the container locations stores a different one of a unique sequence of random number values. The scrambler forms another binary value by rearranging the bits of the input binary value as a function of the random number values in addition to altering the states of such bits as a function of the random number values and the numeric bit position values of the input binary bits. The resulting binary value is applied to an alphanumeric encoder which converts the binary value into series of alphanumeric characters containing a valid key value. In one embodiment, a serial number is used as part of the input binary value.

Applicants respectfully submit that there is nothing in either the Folmsbee or Hirsch reference that teaches or suggests the Applicants' method of authenticating a software application wherein the software application, if being executed on the computer system for the first time, is authenticated *at the computer system and only for that particular computer system using an identifier of the computer system* and if the software application is not being executed for

the first time uses the identifier of the computer system to determine if the computer executing the software application is the computer system for which the software application has been authenticated.

It is clear that Folmsbee teaches to retrieve a key from a remote location that is pre-configured for each CPU. Knowledge of each CPU is therefore required in advance so that the proper keys can be generated. There is nothing in Folmsbee to teach or suggest authenticating a software application at the computer system running the software application, by generating an engraved signature at the computer system using a computer system identifier, when the engraved signature is blank (signifying initial use of the software application). In fact, the teachings of Folmsbee are the exact opposite, namely to pre-create keys necessary to run software applications so that the software applications cannot be run even once without the keys. Hirsch adds nothing to Folmsbee and simply discloses a method of generating a unique key value. Combining Hirsch and Folmsbee would simply result in the Hirsch method being used to generate the pre-created keys stored by Folmsbee. Applicants respectfully submit that any combination of the cited references alleged as resulting in the recitations of claim 16, could only result from an arbitrary selection of prior elements and would disregard the teachings of the prior art considered as a whole.

Accordingly, Applicants respectfully submit that independent claim 16 distinguishes patentably over the cited prior art and should be allowed. As claims 2-5 are dependent either directly or indirectly on an allowable claim 16, Applicants respectfully submit that these claims should also be allowed.

Independent claims 11 and 17 recite subject matter similar to that recited in independent claim 16 and are believed to distinguish patentably over the prior art for the same reasons set forth above. As claims 7-10 are dependent either directly or indirectly on an allowable claim 17, and as claims 12, 13 and 15 are dependent

Application No.: 10/003,538
Final Office Action Dated: February 2, 2005
Response to Final Office Action Dated: January 3, 2006

either directly or indirectly on an allowable claim 11, Applicants respectfully submit that these claims should also be allowed.

In view of the above, it is believed that the application is in order for allowance and action to that end is respectfully requested.

Applicants believe that no additional fees are required, beyond those already paid in connection with the RCE and extension of time. If any additional fees are deemed necessary, please charge Deposit Account No. 13-0235.

Respectfully submitted,

By

Justin R. Sauer
Registration No. 56,920
Agent for Applicants

McCormick, Paulding & Huber LLP
CityPlace II, 185 Asylum Street
Hartford, CT 06103-3402
(860) 549-5290